



El valor de la competencia técnica profesional y la independencia del auditor



En una primera aproximación, puede decirse que el informe de auditoría de sistemas de información es un documento que presenta el trabajo efectuado por el auditor y su opinión profesional sobre la totalidad, área o sección del S.I. objetivo de la auditoría. El informe es, a la postre, el resultado final y formal que refleja todo su esfuerzo comprensivo de los elementos personales, temporales, identificativos de alcance y de opinión, que incluye conclusiones, recomendaciones, salvedades (reservas y calificaciones) y fallos significativos detectados. La finalidad y los usos de dicho informe, sean cuales fueren, justifican la auditoría y su realización por el susodicho auditor, en función de dos de sus atributos capitales: la competencia técnica profesional y la independencia.

José de la Peña Sánchez

Para centrar el asunto del que aquí se trata, conviene fijar algunas definiciones de los conceptos involucrados. La primera que se propone es la de auditoría, y de todas las existentes, se ha seleccionado la contenida en la recientemente traducida al castellano ISO 9000/1999, breve, concisa y de gran calidad. Dice así: «Proceso sistemático independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los criterios de auditoría».

Obviamente, los criterios de auditoría se definen en la misma norma como el «Conjunto de políticas, procedimientos o requisitos contra los que se compara la evidencia de la auditoría».

Si se parte del hecho -quizá discutible- de que quien realiza auditorías de S.I. es un auditor de S.I., sobreviene un problema: que la actividad, profesión u oficio de los auditores de S.I. no están reconocidos en la legislación española. Por tanto, bien cabe apuntar que los auditores de S.I. no existen (oficialmente), pero haberlos, haylos.

Como ya se ha apuntado, el objetivo de la auditoría de S.I. es el Informe, documento inequívocamente vinculado a su autor o autores, convenientemente autenticado, con garantías de integridad y de acceso permitido a quienes estén autorizados, en el que el auditor da su opinión profesional independiente al destinatario. Este informe tiene valor para el auditado, y también en ciertos supuestos y escenarios, para terceros y para organismos de control.

Por ejemplo, el informe de la auditoría que se pide en el Reglamento de medidas de seguridad a partir del nivel medio y en el Artículo 4 Punto 4 (cuya entrada en vigor está prevista para este año, salvo sorpresas), es de utilidad para el auditado y está previsto que pueda ser accedido por la Agencia de Protección de Datos, el órgano de control en la materia. En última instancia, y aunque no tengan acceso, este informe es de interés para los afectados/interesados, cuyos derechos se pretende respetar y proteger.

CLASIFICACIÓN

Las auditorías pueden clasificarse del siguiente modo:

- En función del **sueto**: interna o externa, pública o privada
- En función del **alcance**: totales o completos, parciales o de alcance limitado

• En función del **origen del mandato**: obligatorias o voluntarias

• En función del **objetivo**: S.I., datos personales, calidad, cuentas, fiscal, seguridad e higiene en el trabajo...

• Según el **sector económico**: Industria:..., Servicio:...

De acuerdo con esta clasificación, la auditoría del Reglamento es privada, puede ser interna o externa, su alcance es total en función de las medidas, resulta obligatoria por el origen del mandato y el objetivo viene definido por el tratamiento de datos personales a partir del nivel medio. En relación con el sector económico, afecta de hecho a cualquier entidad de cualquier sector en la que se traten datos personales del nivel correspondiente.

ASESORÍA, CONSULTORÍA, AUDITORÍA E INFORME. PRECISIONES

La confusa situación actual de mercado obliga a precisar algunas cuestiones. La primera de ellas tiene que ver con el informe, que consiste en la opinión técnica profesional del auditor de S.I., y no en un certificado, ya que con él no se asegura la veracidad de un hecho. No distinguir bien este particular es el origen del denominado *audit expectations gap* de algunos usuarios. También es fuente de confusión para algunos ejecutivos poco finos de compañías con auditorías obligatorias de diversa índole.

Bien cabe apuntar que los auditores de S.I. no existen (oficialmente) en España, pero haberlos, haylos

Por otra parte, y más hoy, conviene diferenciar el término auditoría de los de asesoría y consultoría, entre otras razones porque el primero, es decir, la auditoría, está muy estrechamente relacionado con el concepto, polémico en estos días, de independencia y sus correspondientes incompatibilidades entre el auditor (sobre todo si es externo) y el auditado.

En auditoría de S.I., y concretamente en la auditoría del Reglamento, este particular no presenta problema alguno, al no existir por ahora como requisito el de la independencia, ni fijarse incompatibilidades de los auditores (sin regulación oficial), que pueden haber sido antes de la auditoría, y serlo después, asesores o consultores, cosa difícil de encajar en otros

ambientes de doctrina más ortodoxa.

Si se atribuyen al concepto de auditoría de S.I. unas características que lo vinculan con la emisión de una opinión técnica profesional, el examen metódico, independiente y objetivo, las disposiciones (en su sentido más extenso: leyes, usos, normas profesionales...) previamente establecidas, las comprobaciones que se llevan a cabo y la adecuación para llegar al fin previsto..., resulta posible matizar las otras realidades mencionadas, es decir, la asesoría y la consultoría, a la vez tan próximas y tan lejanas.

La asesoría es aquel servicio profesional orientado a conseguir hallazgos y emitir conclusiones o recomendaciones para que el asesorado tome decisiones. El asesor ofrece diversas opciones ante un problema a fin de que el receptor del servicio elija. Suele ser periódica o continua.

Se entiende por consultoría aquel servicio profesional centrado en suministrar consejos sobre asuntos determinados en un periodo de tiempo no muy largo. El consultor ofrece de forma puntual la mejor solución a un problema específico.

Ni qué decir tiene que estas aproximaciones, además de discutibles, están sometidas hoy a fuertes presiones, entre otras razones porque el binomio 'independencia + incompatibilidades' no ha encontrado el punto deseado de coordinación con la oferta de los llamados servicios profesionales (integrales, complementarios...).

ESTADO DEL ARTE

Actualmente existen diferencias entre los EE.UU. y la UE en lo que respecta a la orientación teórica y práctica de la actividad auditora. Desde luego, la globalización y el desarrollo sostenible están acelerando la convergencia, pero todavía las diferencias entre la cultura anglosajona, basada en la *common law*, y la rígida cultura europea continental, en tanto en cuanto no se llegue a una síntesis, han sido, son y serán origen de tensiones e incertidumbre.

Parece ser que la UE preconiza la utilización de las Normas internacionales elaboradas por entidades con participación conjunta (IFAC, IOSCO...), que lentamente unificarán la normativa EE.UU.-UE... No obstante, se detectan procesos de aceleración, ya que todas las multinacionales a partir de un nivel significativo, cotizan en Wall Street/NYSE, en donde la poderosa SEC impone sus normas, basadas en la independencia de los auditores, cuyas consecuencias ya se están dejando notar.

AQUÍ Y AHORA: CÓMO SE ENCUENTRA LA AUDITORÍA DE S.I.

Como antecedentes normativos de las Auditorías de S.I., cabe mencionar a ISACA/OAI, ICAC/IFAC vía directivas UE, y AENOR/ISO vía CEN/CENELEC (UE). No obstante, mientras no exista un reconocimiento oficial del Auditor de S.I., aparecen en opinión de quien esto escribe dos vías posibles de doctrina en primera aproximación: la de la auditoría de cuentas y la de la auditoría de calidad (se deja de lado la auditoría obligatoria relacionada con la seguridad e higiene en el trabajo), ya que el concepto amplio de S.I. permite la utilización del trabajo del Experto Independiente, tal como se define por ISACA/OAI e ICAC/IFAC.

Desde luego, en el caso de una auditoría voluntaria y privada no existe problema en principio; otro cariz tiene, sin embargo, el uso del Informe, que debería estar previsto en el contrato de auditoría o carta de encargo. Este aspecto afecta o puede afectar a los honorarios del auditor, entre otros epígrafes importantes.

La experiencia en auditoría respecto de posibles situaciones conflictivas ante y/o post-Informe, que pudieran tener su origen en la utilización del trabajo de terceros (otros auditores, el auditor interno y el experto independiente) por el auditor externo, recomienda concretar y fijar las condiciones de aprovechamiento y de acceso a los informes y a la documentación (papeles de trabajo).

IRREGULARIDADES Y ERRORES

Este asunto, especialmente conflictivo cuando los fallos son significativos, es el origen remoto del ya mencionado *audit expectations gap* de muchos usuarios.

Se entiende por irregularidad a los actos y omisiones intencionados o negligentes, y por error a los actos y omisiones no intencionados, todos cometidos por uno o más individuos: administradores, dirección, empleados de la entidad auditada, o terceras personas ajenas a ésta que alteren la información auditable.

Parece obvio que la evaluación del control interno es esencial para determinar la realización de pruebas sustantivas, en la medida en que resulta necesario para minimizar el riesgo de auditoría, en vez de las pruebas de cumpli-

miento, todo ello para obtener la evidencia: suficiente, adecuada, relevante, fiable.

Los errores y las irregularidades deben incluirse en el Informe de Auditoría, además de comunicarse a la Dirección de la Entidad lo antes posible, previa valoración de las circunstancias del caso por el auditor. Si éste mantiene dudas sobre los últimos responsables de la gerencia de la entidad auditada, deberá obtener el adecuado asesoramiento legal como ayuda en la determinación de los procedimientos a seguir.

No está claro en todos los casos que la consultoría y la asesoría sean compatibles con la auditoría, especialmente en lo concerniente a las auditorías obligatorias, incluso si se crean sociedades diferentes dentro del grupo

Este punto es delicado en cualquier auditoría; igualmente en la de S.I. y de Reglamento, que debido a sus características actuales (no hay regulación, no hay reconocimiento oficial del auditor...) pueden ser encargadas por el primer ejecutivo de la entidad, por el DSI o por un directivo de inferior rango con poderes para ello.

GLOBALIZACIÓN, FUSIONES Y AUDITORÍA

Interesa recordar que en el Foro de Davos 2000 se ha mencionado que el dilema sobre el

desarrollo de Internet se encuentra entre la Tecnología y los Contenidos. Efectivamente, en los S.I. existen ambos componentes, que son polifacéticos (también los recursos humanos, los grandes olvidados), y ello da que pensar ante el hecho de que en menos de medio siglo se ha pasado de los sistemas manuales al Proceso de Datos/Informática (términos casi equivalentes), y de ahí al complejo TICs-S.I. A esto se suma el fenómeno de crecimiento de las grandes corporaciones, que ha provocado una especie de fusión-manía («*caballo grande, ande o no ande*») de consecuencias serias para el control y, lógicamente, para la auditoría, máxime en campos nuevos como es, a efectos reglamentarios, el del tratamiento de los datos personales.

Para aprovechar las oportunidades y dar curso a la cobertura de las necesidades crecientes, las por el momento *big five*, que empezaron como auditoras, ofrecen mediante sus equipos multidisciplinares de formación generalista/especialista (conocer todo de todo) servicios profesionales globales, incluida la externalización de funciones, fenómeno en parte motivado por la congelación/disminución del mercado específico de auditorías de cuentas, y por la lógica tendencia a abrir y a no dejarse arrebatar otros mercados rentables.

Sin embargo, el péndulo se encuentra hoy en el otro extremo, tanto en Estados Unidos como en la UE, que consideran como esencial para el sistema mantener la competencia. Por tanto, la independencia profesional tiene y va a



tener connotaciones muy estrictas, y no está claro en todos los casos que la consultoría y la asesoría sean compatibles con la auditoría, especialmente en lo concerniente a las auditorías obligatorias, incluso si se crean sociedades diferentes dentro del grupo.

CORPORATE GOVERNANCE: LOS INFORMES OLIVENCIA

El llamado Buen Gobierno de las Corporaciones, procedente de EE.UU. especialmente, no ha llegado por parte de la UE, en la que la Quinta Directiva del derecho de Sociedades sigue hibernada en Bruselas. Pero los informes UK Cadbury-Greenbury-Hampel sí han influido en España vía el Informe Olivencia I, que afecta sensiblemente a los sistemas de información y a la auditoría.

Para mensurar el alcance de lo dicho puede mencionarse que en el primer Informe (puesto que el segundo está aún en proceso de elaboración), se indica que entre el núcleo de facultades indelegables de los consejos de administración, se encuentra:

- La identificación de los principales riesgos de la sociedad
- La implantación y seguimiento de los sistemas de control interno y de información adecuados.

Además, recomienda (sólo recomienda) la existencia de Comisiones de Auditoría con la participación de Consejeros Independientes. Las actividades de dichas Comisiones, podrían favorecer la desaparición de las salvaduras en los informes de la auditoría externa.

COMPETENCIA PROFESIONAL E INDEPENDENCIA

Ante la proliferación de auditorías especializadas, resulta coherente la oferta y la demanda de servicios integrales. De hecho, esa es la tendencia en algunas corporaciones. Sin embargo, en auditoría, el tema básico, el meollo del asunto, gira alrededor de dos de los atributos del auditor, que son la base de su razón de

ser. Sin ellos no hay auditor ni auditoría tal y como cabalmente se conocen:

- **La Competencia Técnica Profesional**, que reside en la capacidad para detectar irregularidades y errores
- **La Independencia**, que es la disposición a reflejar en el Informe de Auditoría todos los problemas y los defectos que haya detectado.

LA AUDITORÍA Y EL REGLAMENTO DE MEDIDAS DE SEGURIDAD

El Reglamento de medidas de seguridad es un buen texto normativo, que ofrece unas expectativas tentadoras para los auditores de S.I. (que repetimos, no existen oficialmente): obliga a una auditoría privada, ya interna o externa, marca plazos límite para hacerla, e indica su objetivo: el tratamiento de los datos personales...

Lo que no queda tan claro es su alcance, debido a las implicaciones organizativas del asunto; por añadidura, no hay una experiencia auditora, ni interna ni externa, en la obtención de evidencias, ni para las duras, es decir, aquellas observables y verificables; ni para las blandas, que son observables pero no verificables. No hay histórico, salvedad hecha de las específicamente realizadas en el pasado por mandato de la Agencia en la Instrucción relativa a los habitualmente denominados ficheros de morosos de uso en entidades financieras y de crédito.

El Reglamento de medidas de seguridad ofrece unas expectativas tentadoras para los auditores: obliga a una auditoría privada, ya externa ya interna, marca plazos límite para hacerla e indica su objetivo: el tratamiento de los datos personales

Además, los conceptos de competencia técnica profesional e independencia no han sido considerados, por lo que hay gran libertad de acción para externos de asesoría y consultoría. El asesor (interno o externo) que nos asesore, y el consultor (interno o externo) que nos ayude a adaptarnos al nivel medio (en tanto que próximo hito), podrá auditarnos.

Todo indica que la intención del legislador, más allá de cualquier consideración, ha sido fomentar la existencia de una política, de unas normas, de su control, y, finalmente, de una función, la de auditoría, que verifique controles, detecte problemas y dé alternativas. *Chapeau*. A eso se llama empezar la casa por los cimientos. Una vez que la casa esté construida, habrá que estudiar si el concepto de auditoría vigente debe cambiar a criterios más cerrados desde el punto de vista regulador. O no.

El Artículo 38 de la Constitución, que versa sobre la libertad de empresa en el marco de la economía de mercado, orienta al Reglamento en su Artículo 17, ya que es potestad del responsable del fichero designar al auditor, tanto si es interno como si es externo.

Ahora bien, respecto a la función de auditoría interna, conviene precisar que el mercado actual ofrece un amplio abanico de soluciones, que se encuentran entre la auditoría interna adscrita a la plantilla del personal de la propia entidad y la externalización total de la función,

PUNTOS BÁSICOS PARA LA ELABORACIÓN DE UN INFORME DE AUDITORÍA DE S.I.

Se relacionan a continuación los puntos más importantes a la hora de realizar un Informe de auditoría de S.I., según ISACA:

- ANTECEDENTES
 - Correspondencia normativa
 - Necesidad de Guía
- INFORME
 - Propósito y contenido
 - Receptores designados
 - Estilo y contenido
 - Declaración de objetivos
 - Ámbito, naturaleza, tiempo y extensión del trabajo
 - Restricciones en la distribución
 - Fallos significativos
 - Conclusiones
 - Recomendaciones
 - Reservas y calificaciones
 - Presentación
 - Oportunidad
 - Consideraciones de los sucesos posteriores
- ACTIVIDADES POSTERIORES
 - Solicitud de respuesta

admitiendo la gradación adecuada en el tiempo y en el espacio a las necesidades cambiantes. Bien podría decirse aquí que «*más sabe el loco en su casa que el cuerdo en la ajena*».

En lo que concierne a la auditoría externa, y aunque ya se ha comentado mucho, quizá merezca la pena resaltar que el Informe, que debe «*incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas*», quedará a disposición de la Agencia de Protección de Datos. Si ésta accediera a los informes que se elaboren, el Director del órgano de control estaría en una inmejorable posición para decidir, si lo considera oportuno, sobre su calidad y adecuación al objetivo. El futuro dirá.

Para finalizar, es importante tratar un asunto que puede convertirse en espinoso si no se tiene en especial consideración y si, además, la tecnología para el tratamiento y la gestión de datos se implanta sin atender a leyes y requisitos normativos. Nos referimos al Artículo 4 del Reglamento, «*Aplicación de los niveles de seguridad*», Punto 4: «*Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20*».

Estos ficheros (los tradicionales y los tratados en los emergentes entornos y servicios web), que podrían utilizar permanentemente las E.T.T. (empresas de trabajo temporal), las consultoras conocidas como «*head hunters*», e incluso las BB.DD. y los almacenes de datos de Potencial Humano de las empresas, deberían ser objeto de especial atención, ya que forman un activo inmaterial estratégico con su correlativa Gestión del Conocimiento, expresiones estas últimas que son desde hace tiempo los pétalos de la más joven flor nacida en los fértiles jardines del *tecno-consulting* desmemoriado. ■

JOSÉ DE LA PEÑA SÁNCHEZ

Auditor Censor Jurado de Cuentas
y Licenciado en Informática
Correo-e: codasic@jet.es

ESQUEMA SIMPLIFICADO DE UNA AUDITORÍA TIPO

A continuación, se enumeran los eventos más significativos a la hora de realizar una auditoría.

- a) INICIACIÓN: contactos iniciales
- b) INFORMACIÓN PRELIMINAR:
 - Conocimiento de la entidad y el sector
 - Evaluación del riesgo de auditoría y del control interno
- c) CONTRATO DE AUDITORÍA o carta de encargo
- d) CARTA DE MANIFESTACIONES DE LA DIRECCIÓN
- e) PLANIFICACIÓN: determinación de pruebas de cumplimiento y sustantivas
- f) PROGRAMACIÓN: distribución de recursos y tareas en el tiempo
- g) REALIZACIÓN: obtención, documentación y evaluación de la evidencia
- h) RAZONAMIENTO:
 - Detección de fallos (errores y fraudes) y su evaluación
 - Concreción de salvaduras (alcance y/o incertidumbre)
 - Elaboración de recomendaciones
- i) INFORME: conclusiones - OPINIÓN TÉCNICA PROFESIONAL
- j) DISTRIBUCIÓN